MIS 4596

Milestone 4 Guidance

Milestone 4 instructions

Your assignment is to transform your Milestone 3 penetration test and vulnerability identification report into a **vulnerability identification and security mitigation and control ("remediation") report**

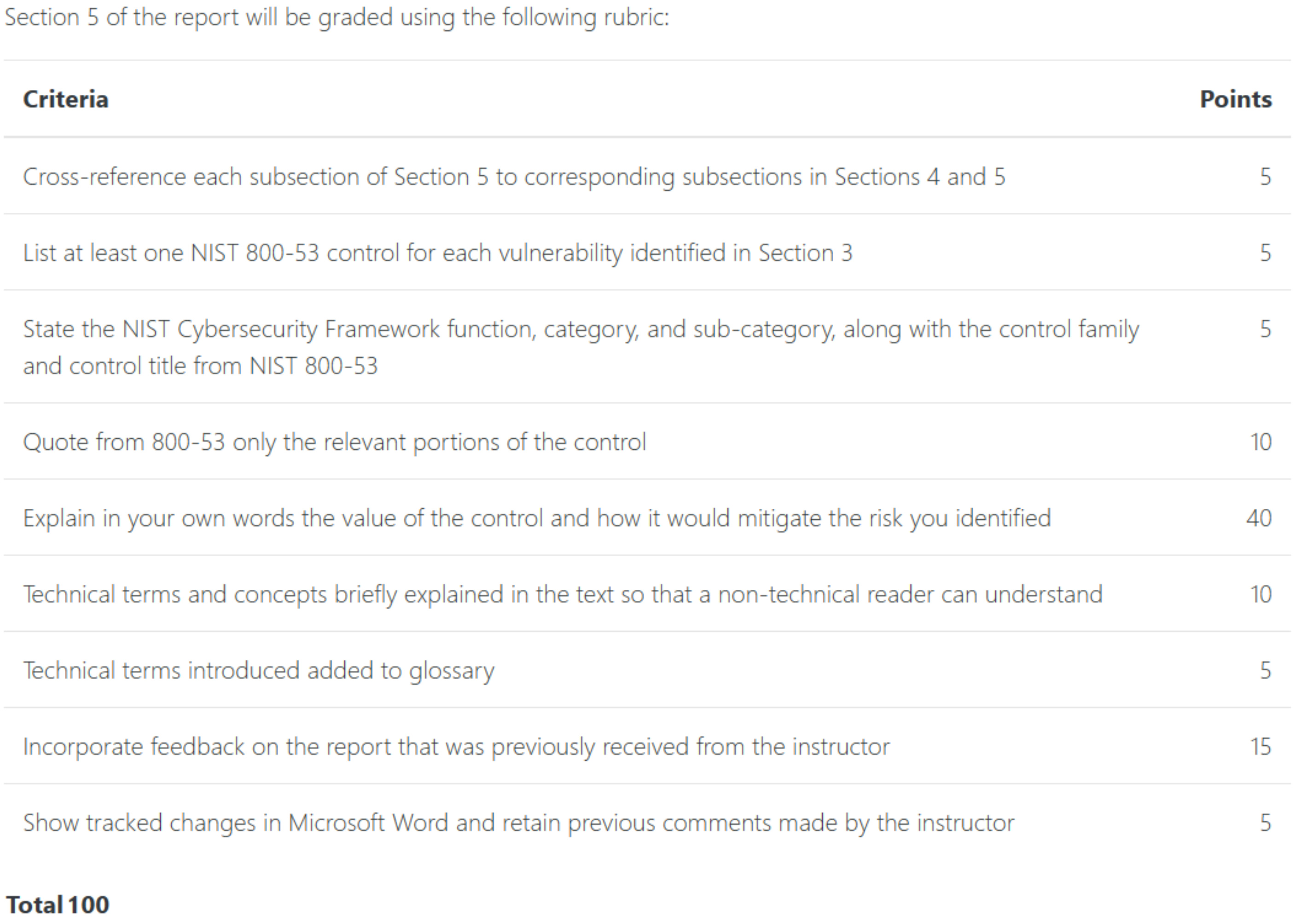
As before, your report is for senior managers of the company who owns and depends on information stored on and processed within the server you examined in your penetration test

Be sure your report

1. Clearly identifies:
   - The level of concern the managers should have for confidentiality, integrity, and availability of the information on the server
   - The potential impact on the business' assets, operations, and people should the information and information system be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction
2. Identifies the vulnerabilities you found during your penetration test
3. Recommend information security controls for mitigating each of the vulnerabilities you found

Milestone 4 Grading Rubrics

	Section	Points
	Executive Summary	10.0
1	Project Scope	2.5
2	Target of Assessment	2.5
3	Relevant Findings	15.0
4	Supporting Details	15.0
5	Vulnerability Remediation	50.0
6	Glossary	2.5
7	References	2.5
	Total:	100.0



Section 5 of the report will be graded using the following rubric:

Criteria	Points
Cross-reference each subsection of Section 5 to corresponding subsections in Sections 4 and 5	5
List at least one NIST 800-53 control for each vulnerability identified in Section 3	5
State the NIST Cybersecurity Framework function, category, and sub-category, along with the control family and control title from NIST 800-53	5
Quote from 800-53 only the relevant portions of the control	10
Explain in your own words the value of the control and how it would mitigate the risk you identified	40
Technical terms and concepts briefly explained in the text so that a non-technical reader can understand	10
Technical terms introduced added to glossary	5
Incorporate feedback on the report that was previously received from the instructor	15
Show tracked changes in Microsoft Word and retain previous comments made by the instructor	5

Total 100

What types of controls can you think of to research and include in your report to mitigate the vulnerabilities you found…

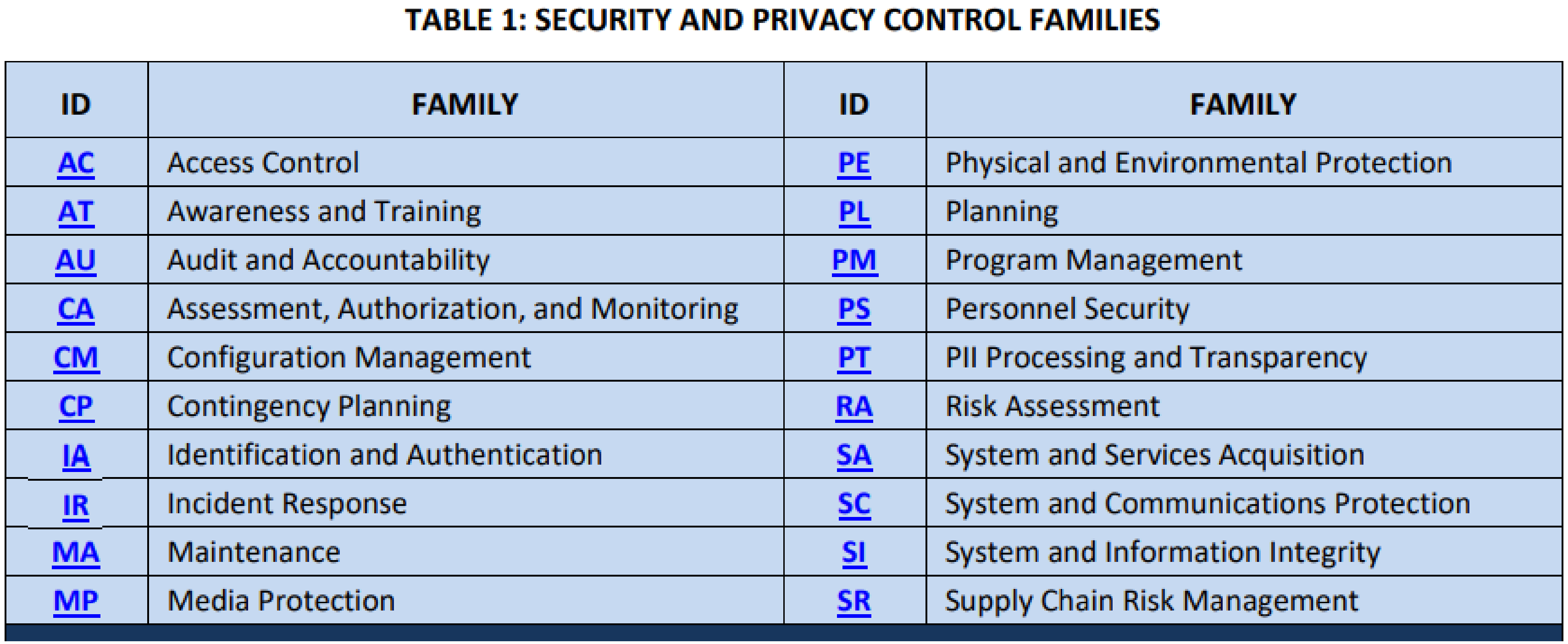
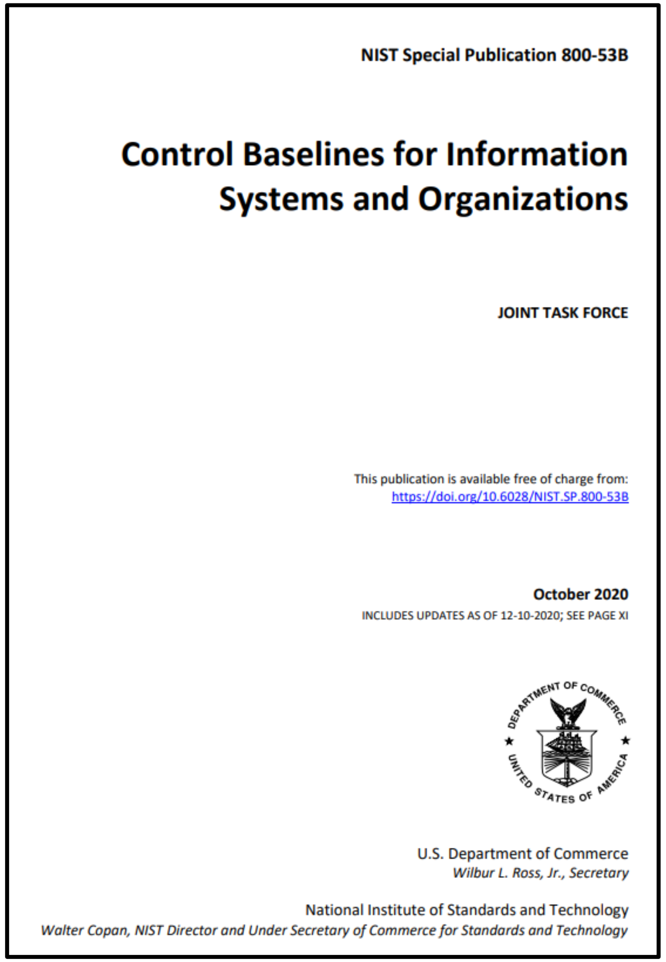


TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Finding Controls to Mitigate Vulnerabilities



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

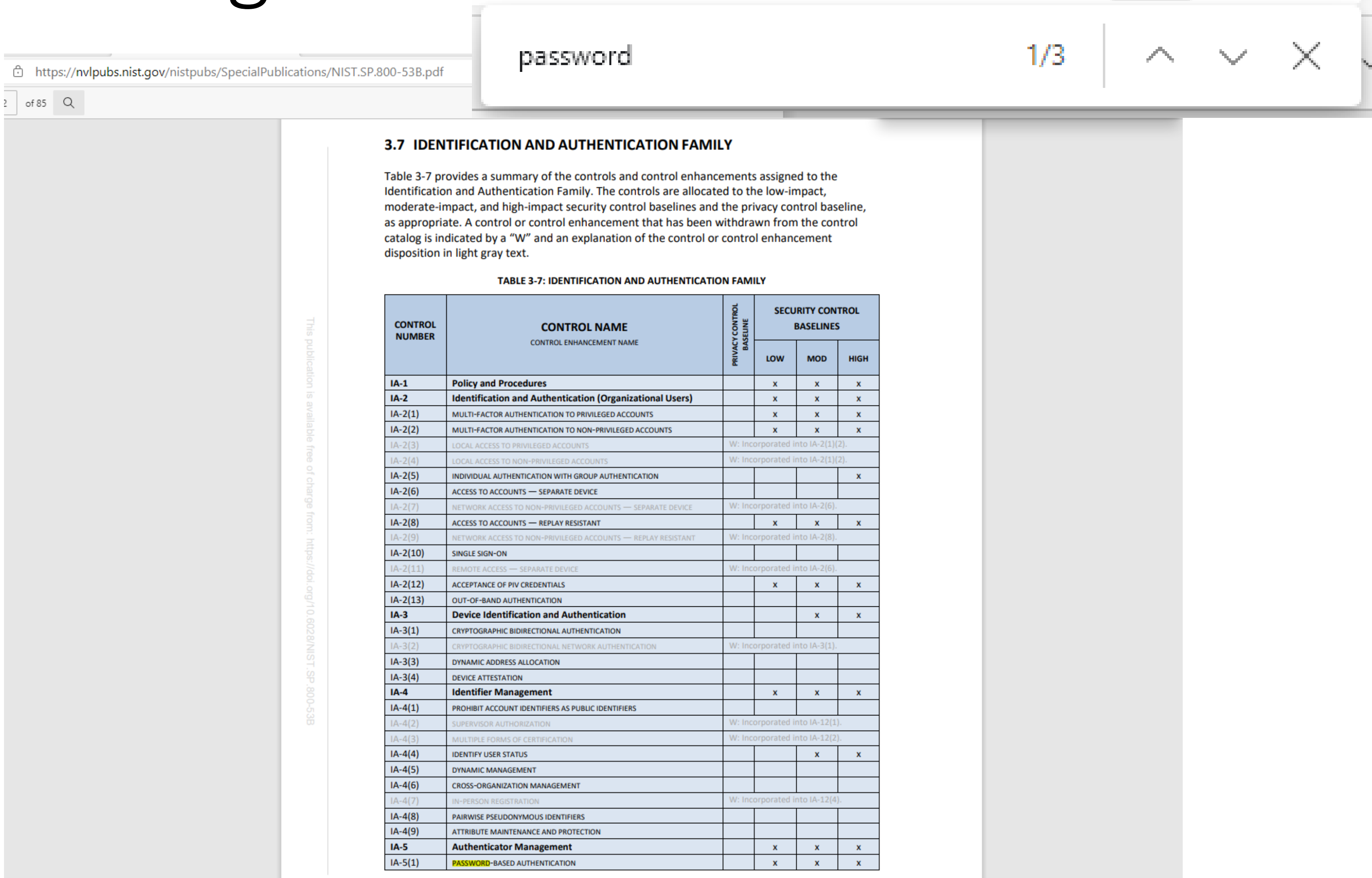
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



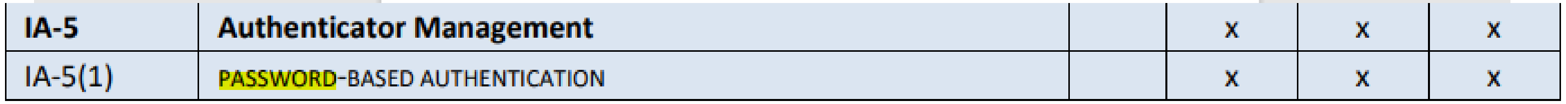
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

3.7 IDENTIFICATION AND AUTHENTICATION FAMILY

Table 3-7 provides a summary of the controls and control enhancements assigned to the Identification and Authentication Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

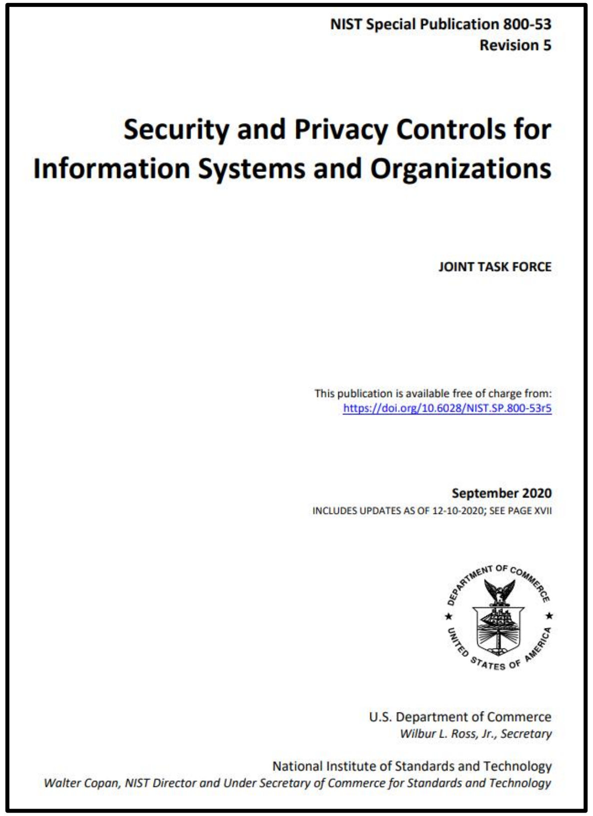
TABLE 3-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-1	**Policy and Procedures**		x	x	x
IA-2	**Identification and Authentication (Organizational Users)**		x	x	x
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE				
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	W: Incorporated into IA-2(8).			
IA-2(10)	SINGLE SIGN-ON				
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION				
IA-3	**Device Identification and Authentication**			x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION				
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W: Incorporated into IA-3(1).			
IA-3(3)	DYNAMIC ADDRESS ALLOCATION				
IA-3(4)	DEVICE ATTESTATION				
IA-4	**Identifier Management**		x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS				
IA-4(2)	SUPERVISOR AUTHORIZATION	W: Incorporated into IA-12(1).			
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	W: Incorporated into IA-12(2).			
IA-4(4)	IDENTIFY USER STATUS			x	x
IA-4(5)	DYNAMIC MANAGEMENT				
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT				
IA-4(7)	IN-PERSON REGISTRATION	W: Incorporated into IA-12(4).			
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS				
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION				
IA-5	**Authenticator Management**		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x



IA-5	**Authenticator Management**		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x

Example of Control to Mitigate a Vulnerability…



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

IA-5 **AUTHENTICATOR MANAGEMENT**

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

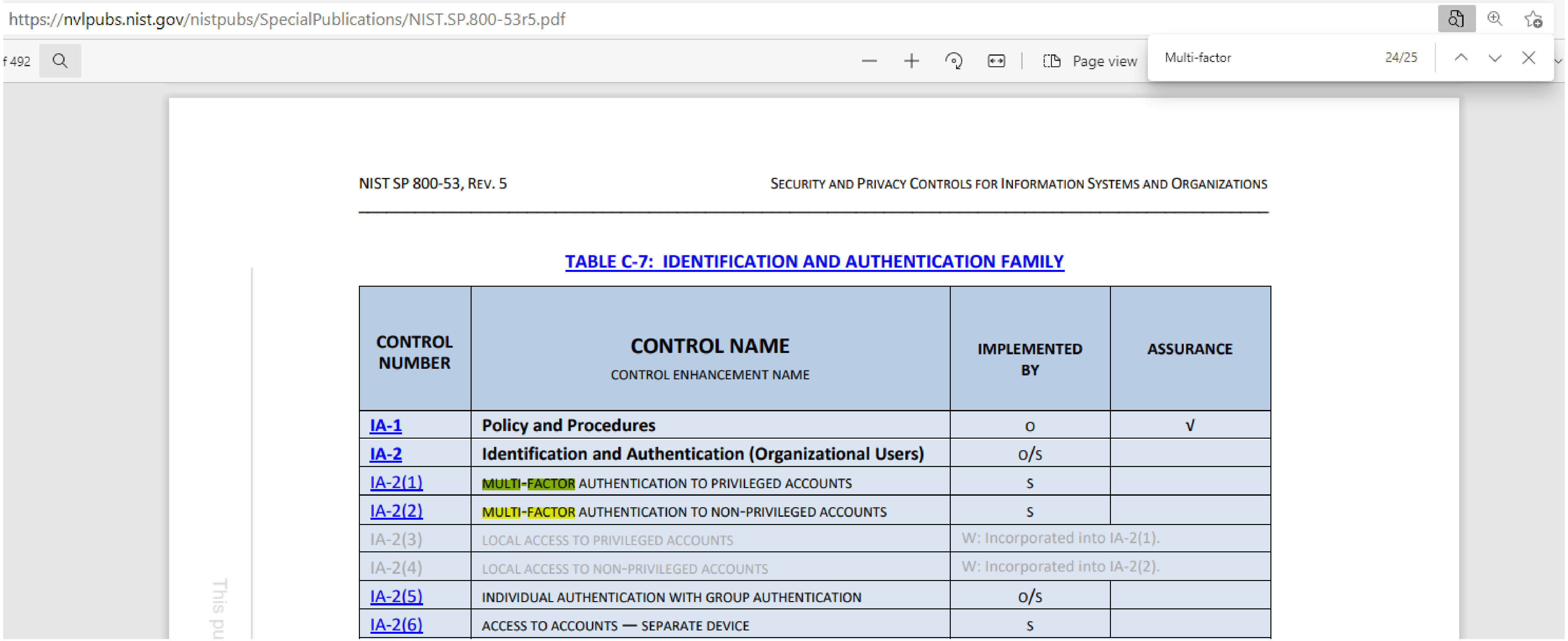
(h) Enforce the following composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*].

Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Related Controls: IA-6.

Read and understand what this control is about, identify the basic information you need for your report

Search NIST SP 800-53 for additional controls



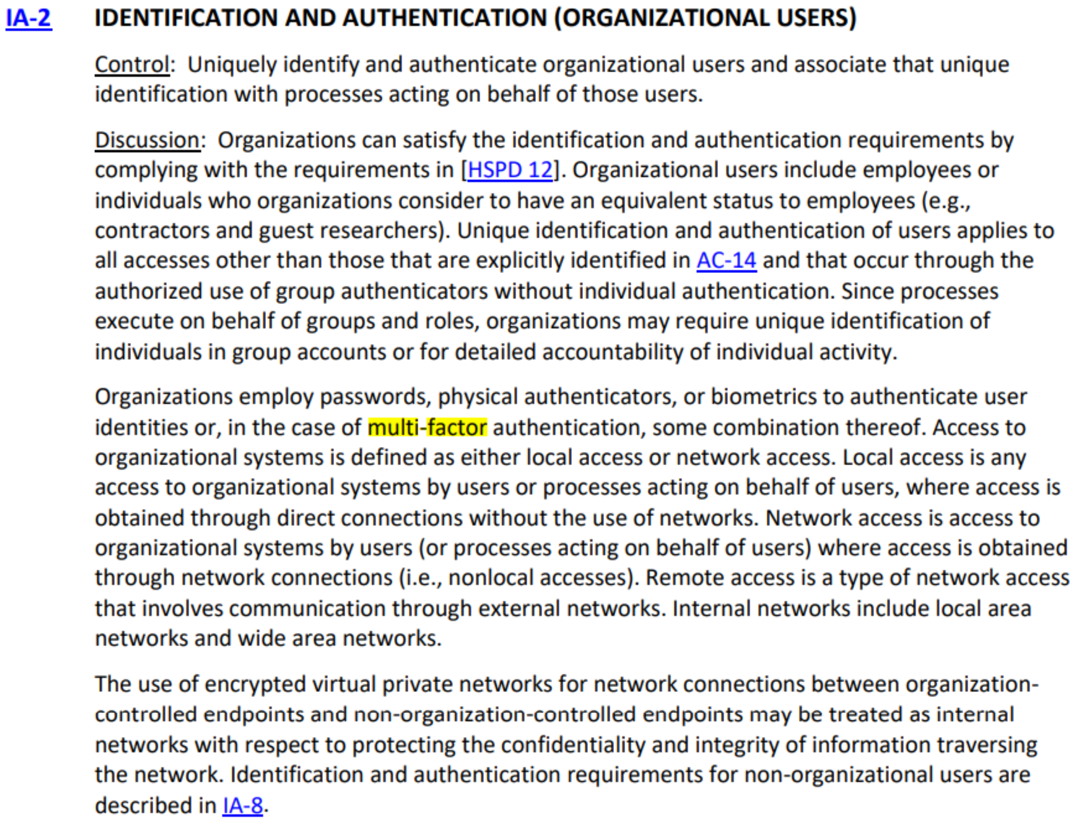
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
f 492
Page view
Multi-factor
24/25
This pu

NIST SP 800-53, REV. 5 SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

TABLE C-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	IMPLEMENTED BY	ASSURANCE
IA-1	**Policy and Procedures**	O	√
IA-2	**Identification and Authentication (Organizational Users)**	O/S	
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	S	
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	S	
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1).	
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(2).	
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION	O/S	
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE	S	

Research controls, study the details, then identify the control and summarize briefly in your report



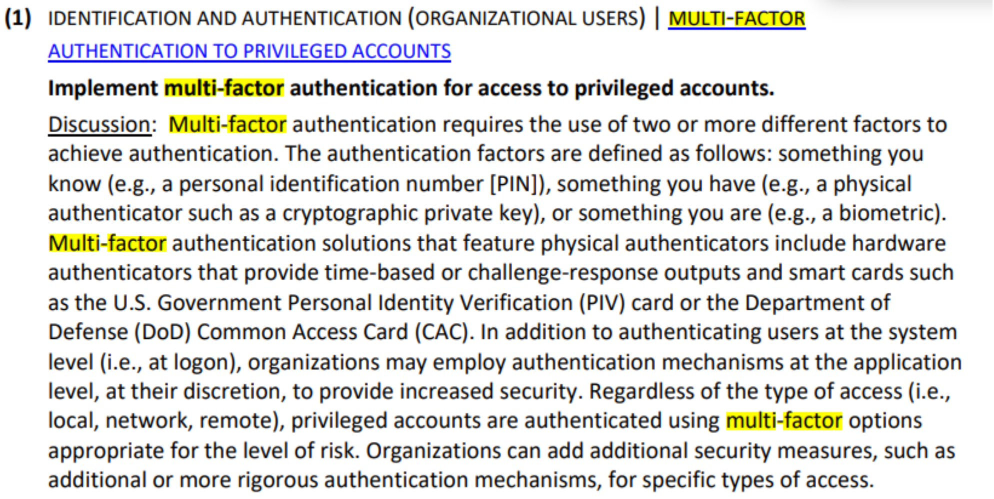
IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

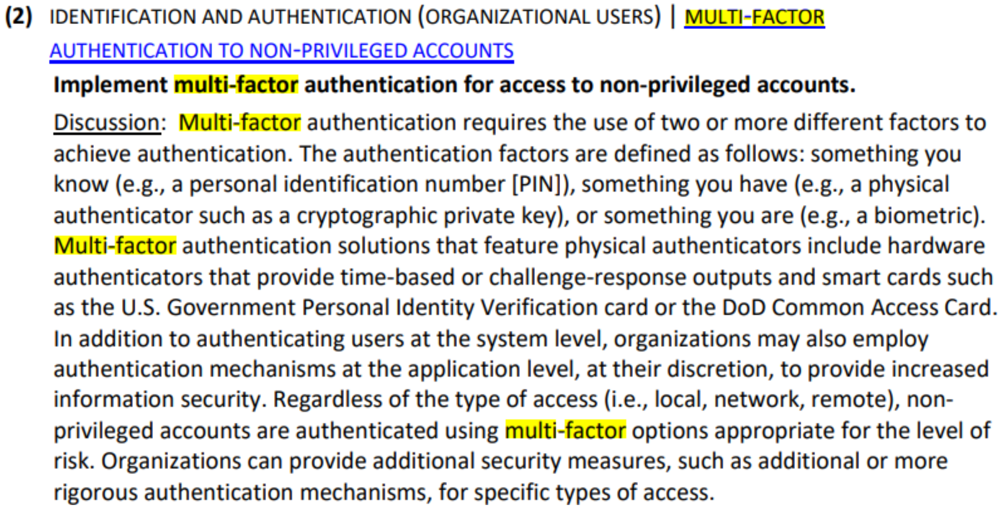
The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.



(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.



(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to non-privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

What other types of controls can you think of to research and include in your report to mitigate the vulnerabilities you found…

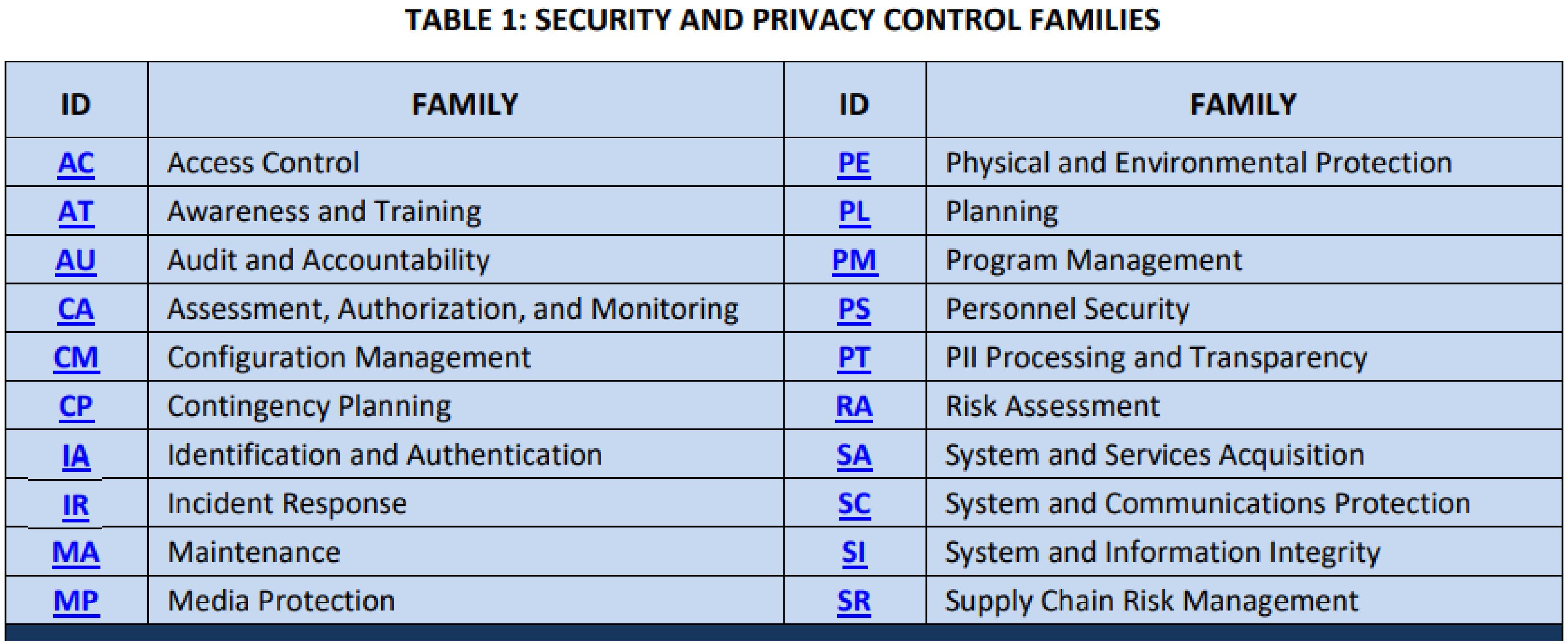


TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Research controls, study the details, then identify the control and summarize briefly in your report

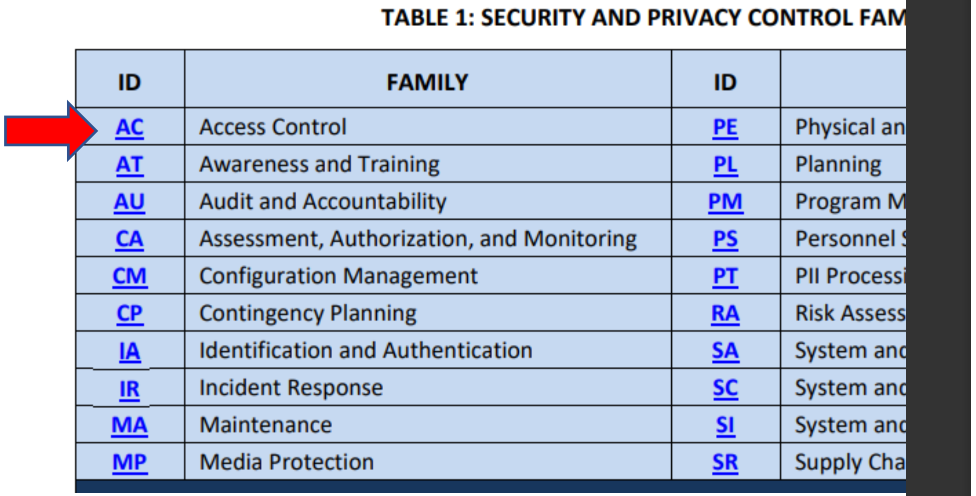
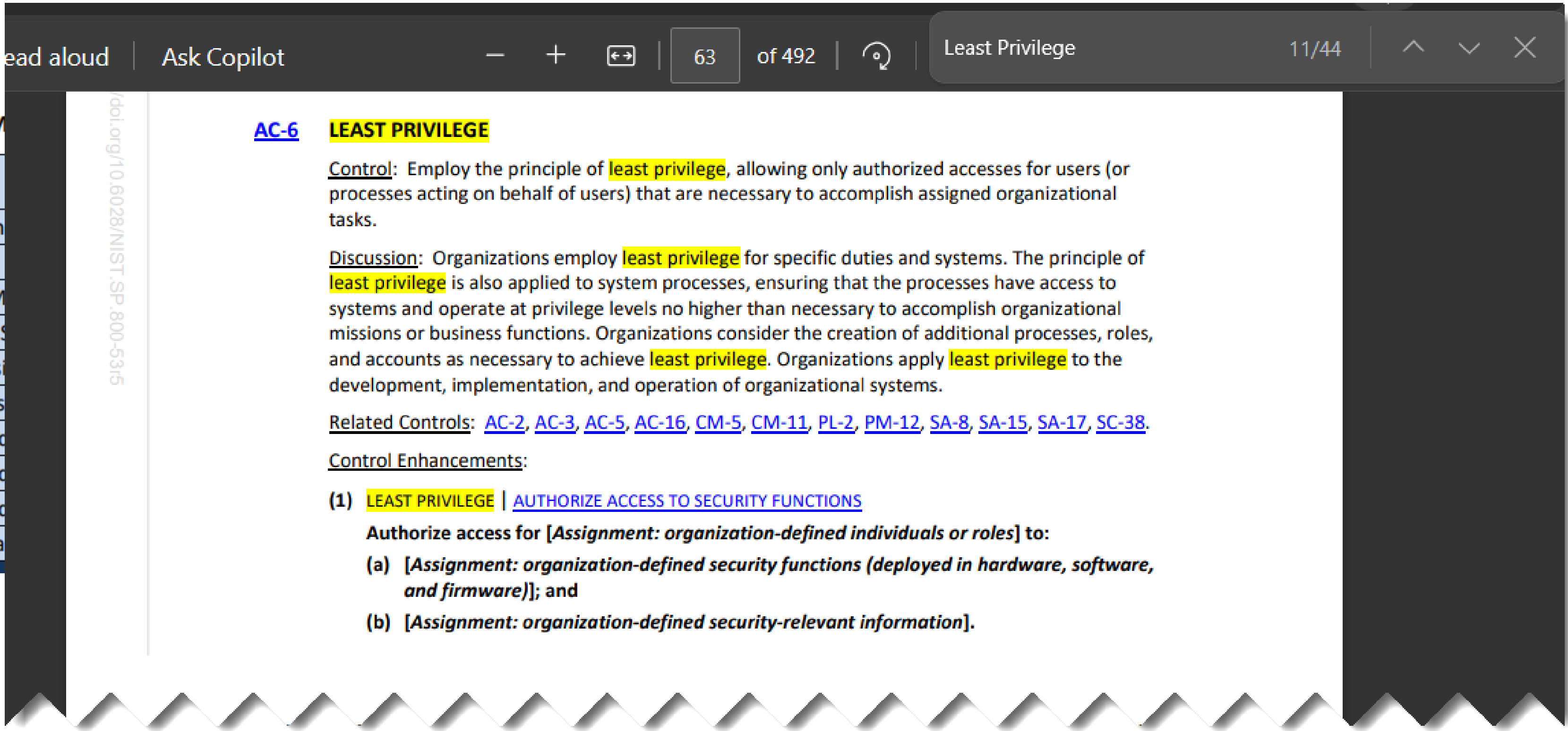


TABLE 1: SECURITY AND PRIVACY CONTROL FAM

ID	FAMILY	ID	
AC	Access Control	PE	Physical an
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program M
CA	Assessment, Authorization, and Monitoring	PS	Personnel S
CM	Configuration Management	PT	PII Processi
CP	Contingency Planning	RA	Risk Assess
IA	Identification and Authentication	SA	System and
IR	Incident Response	SC	System and
MA	Maintenance	SI	System and
MP	Media Protection	SR	Supply Cha



AC-6 LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

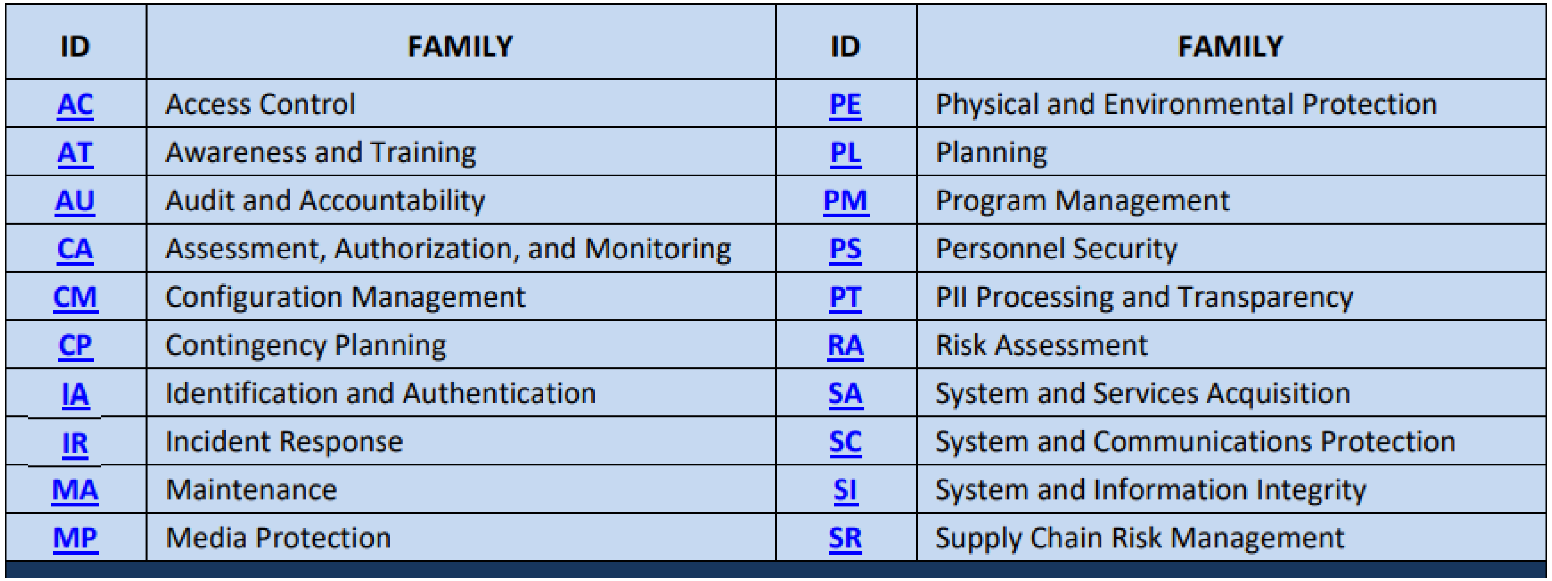
Authorize access for [*Assignment: organization-defined individuals or roles*] to:

(a) [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware)*]; and

(b) [*Assignment: organization-defined security-relevant information*].

What other controls are relevant to mitigate your findings of vulnerabilities?

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management